

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY

**As rescanning documents *will not* correct
images, please do not report the images to the
Image Problem Mailbox.**

⑩ 日本国特許庁 (JP)

⑪ 特許出願公開

⑫ 公開特許公報 (A)

平2-199561

⑬ Int. Cl. 5

G 06 F 12/14

識別記号 庁内整理番号

320 A 7737-5B

⑭ 公開 平成2年(1990)8月7日

審査請求 未請求 請求項の数 9 (全7頁)

⑮ 発明の名称 許可を得ていない保護データ検出に対する安全装置

⑯ 特 願 平1-293759

⑰ 出 願 平1(1989)11月10日

優先権主張 ⑯ 1988年11月10日 ⑮ フランス(FR) ⑯ 88 14707

⑲ 発明者 セルジュ フリュオ フランス国 13790 ベニエ リュ デ ローリエ 4

⑲ 発明者 ローラン スウルジヤ フランス国 13100 エクス サン プロヴァンス シュ
ン マン デュ ベルヴエデール (番地なし)

⑳ 出願人 エスジエーエーストム フランス国 94250 ジャンティイ アヴニユ ガリエニ
ソン ミクロエレクト 7
ロニクス エス.ア

㉑ 代理人 弁理士 越場 隆

明細書

1. 発明の名称

許可を得ていない保護データ検出
に対する安全装置

2. 特許請求の範囲

(1) 集積回路形式のメモリの機密データ保護のための回路であって、制御信号に応じて異なる2つの電流消費状態をとり、個別に制御される複数個のシミュレーションセルと、それらシミュレーションセルが擬似乱数的に上記異なる2つの電流消費状態の一方の状態または他方の状態をとるよう上記シミュレーションセルを制御する擬似乱数発生器とを同一集積回路上に備え、集積回路の総電流消費の読み取りによる機密情報の測定を困難にしたことを特徴とする保護回路。

(2) 上記シミュレーションセルが、上記2つの電流消費状態において、メモリセルとほぼ同じ電流

を消費し、上記2つの電流消費状態の内の第1の状態が、“0”の論理状態にあるメモリセルの電流消費に対応し、上記2つの電流消費状態の内の第2の状態が、“1”の論理状態にあるメモリセルの電流消費に対応することを特徴とする請求項1記載の保護回路。

(3) 上記シミュレーションセルが、メモリセルを形成するトランジスタと同じトランジスタであることを特徴とする、記憶された情報の読み出しに対してメモリを保護するための請求項1または2に記載の保護回路。

(4) 上記シミュレーションセルの各々がフローティングゲートトランジスタで形成され、該トランジスタのフローティングゲートおよび制御ゲートは短絡されていることを特徴とする、機密情報の読み込み時にEEPROMまたはEEPROMを保護するための請求項1または2に記載の保護回路。

(5) 上記擬似乱数発生器が、カスケード接続されたフリップフロップから形成され、該フリップフロップのいくつかの出力が排他的ORゲートを介して入力に戻されてループを構成していることを特徴とする請求項1または2に記載の保護回路。

(6) 上記擬似乱数発生器が、クロック周波数により制御され、該周波数の変化は擬似乱数であることを特徴とする請求項1または2のいずれか一項に記載の保護回路。

(7) いくつかの周波数制御入力をもつ制御周波数発振器を備え、これらの入力が、上記擬似乱数発生器の出力に接続されることを特徴とする請求項6記載の保護回路。

(8) 上記シミュレーションセルの各々が、D型フリップフロップの出力により制御され、該D型フリップフロップの各々が、第1の入力として共通信号を受け、第2の入力として上記擬似乱数発生

器の各出力を受けることを特徴とする請求項1または2に記載の保護回路。

(9) 上記シミュレーションセルの各々がトランジスタを含み、このトランジスタは、保護しようとするメモリを構成する集積回路の給電端子VccとVssの間に、動作禁止トランジスタと直列接続されていることを特徴とする請求項1または2に記載の保護回路。

3. 発明の詳細な説明

産業上の利用分野

本発明は、集積回路に収納された機密情報の安全に関する。

従来の技術

いくつかの集積回路利用装置、より具体的には「チップカード」または「ICカード」として知られるカードに含まれる回路では、許可を得ていない人間が回路のメモリ中に記憶された機密情報

- 3 -

にアクセスするのを防止する必要がある。

この機密情報は、例えば読出し専用メモリ(ROM)または電気的にプログラム可能な不揮発性の読出し専用メモリ(E PROMまたはEEPROM)中に記憶されている。

勿論、この情報を実際にアクセス不可能にするためには、メモリ中に記憶されたデータは集積回路の入出力端子に与えられるべきではない。そのため実際には、機密度が特に高いとき、機密情報は、メモリと同じ集積回路中に含まれるマイクロプロセッサにより処理される。従って、情報は、集積回路内でマイクロプロセッサとメモリとの間を循環するが、集積回路へのアクセス用外部端子には到達しない。この防止法は情報の読出しに関するものである。情報はマイクロプロセッサにより読み出され、利用されるが、マイクロプロセッサは情報を外部に伝送することはない。この防止法はまた、電気的にプログラム可能なメモリの場合、メモリ中の情報の書き込みにも関する。すなわち、マイクロプロセッサは、それ自体が決定した情報

- 4 -

部分を書き込むが、その決定モードはユーザには知られず、書き込まれた情報部分はいかなる時点でも外部端子に現れない。

発明が解決しようとする課題

しかし、迂遠な方法であるが、少なくとも部分的にメモリの内容にアクセスすることが可能であることは知られている。この方法は、メモリの読み出し動作、または書き込み動作の間、集積回路の消費電流を測定することである。

事実、「0」ビットの読み出し動作で消費する電流量は、「1」ビットの読み出し動作で消費する電流量と同じではない。同じことが書き込み動作にも言える。メモリが8ビットのワード単位で読み出されるあるいは書き込まれると、8つの「0」ビットの読み出し(または書き込み)と、8つの「1」ビットの読み出し(または書き込み)との差は、1ビットの読み出し(または書き込み)での差より大きい。

例えば、対象とするビットのアドレスにトランジスタが存在するかしないかにより符号化されだ

読み出し専用メモリの場合には、1つのメモリビットの読み出しは“1”ビットでは200マイクロアンペアを消費するが、“0”ビットでは電流を消費しない。EEPROMまたはEEPROMについても、読み出しおよび書き込みの両方で同様のことが言える。その結果、メモリの読み出しおよび書き込みの間に消費される電流を測定することにより、このメモリの機密内容を一部もしくは全部解読することが可能になる。不正を行おうとするユーザは、給電端子（必然的に集積回路の外からアクセス可能である）間で消費された電流を測定することができる。

機密情報の読み出しの不正行為の例として、集積回路の読み出し専用メモリに記憶された機密プログラム、あるいは、電気的にプログラム可能な回路のメモリに記憶され機密である可能化コードの読み出しが挙げられる。

機密情報の読み出しへはなく、書き込みに関する不正の例としては、次のようなものがある。いくつかの保護されている回路で、ユーザは、その回路

を使用したいとき必ずキーボードを通して可能化コードを入力しなければならないという対策が施されている。あらゆる可能なコードを系統的に入力しての不正を防止するために、間違ったコードが入力されたら必ずメモリにエラービットを記憶するという方法がある。エラーが3つ続くと、3つのエラービットが回路動作を中止させる。しかし、ここでも、電流の消費量を検出し、これによってエラービットが記憶されたことを検出することができる。このような知識は、エラービットの記憶を即座に中断するために使用され、間違ったコードが連続して入力されたとき、ユーザに知られることなく3つのエラービットが記憶されて行われる保護を無効にすることができる。

本発明は、主に、機密情報の読み出し、また場合によっては書き込みにおいて以上のような不正行為の可能性を防ぐことを目的とする。

課題を解決するための手段

本発明は、集積回路形式のメモリの機密データ

- 7 -

保護のための回路であって、制御信号に応じて異なる2つの電流消費状態をとり、個別に制御される複数個のシミュレーションセルと、それらシミュレーションセルが擬似乱数的に上記異なる2つの電流消費状態の一方の状態または他方の状態をとるよう上記シミュレーションセルを制御する擬似乱数発生器とを同一集積回路上に備え、集積回路の総電流消費の統取りによる機密情報の測定を困難にしたことを特徴とする保護回路を提供する。

上記構成により、回路の外部端子から読み取ることができる電流消費は、メモリセルの実際消費と、保護回路のセルの擬似乱数的消費とを重ねたものとなる。

シミュレーションセルは、上記異なる2つの電流消費状態において、メモリセルの電流消費とほぼ等しい電流を消費するように構成することが望ましい。第1の状態は、メモリの“0”ビットでの消費に、第2の状態は、“1”ビットでの消費に対応する。従って、検出はさらに難しくなる。

- 8 -

記憶された情報の読み出しに対してメモリを保護するべきか、あるいはメモリに書き込まれる情報の検出に関して保護するべきかに応じて、シミュレーションセルの設計が異なるのは明らかである。というのは、電流消費値は読み出しおよび書き込みで同一ではないからである。

読み出しに対する保護装置の場合には、シミュレーションセルは、メモリセルを形成するトランジスタと同一のトランジスタから構成する。書き込み中の情報検出に対する保護装置の場合には、シミュレーションセルはフローティングゲートトランジスタにより形成する。このフローティングゲートトランジスタのフローティングゲートおよび制御ゲートは短絡される。

擬似乱数発生器は、カスケード接続されたフリップ・フロップ列により標準的な方法で構成することができる。いくつかのフリップフロップの出力は、排他的ORゲートを介して他のフリップフロップの入力に接続されてループを構成する。

乱数の特徴は、これらのフリップフロップを制

- 9 -

-465-

- 10 -

御するクロック周波数をランダムに変化させることによりさらに高めることもできる。

本発明のその他の特徴および利点は、添付の図面を参照にして行う以下の詳細な説明により明らかにされるであろう。

実施例

第1図に示した本発明に従う保護回路は、保護しようとする回路と同じ集積回路基板上に構成され、同じVcc(高レベル)とVss(低レベル)給電端子により給電される。本発明に従う保護回路は、いくつかのシミュレーションセル(ここでは3つのセル)を具備しており、これらのシミュレーションセルは、それぞれD型フリップフロップを介して、すなわち、第1セルはD型フリップフロップBD1を介して、第2セルはD型フリップフロップBD2を介して、第3セルはD型フリップフロップBD3を介して、擬似乱数発生器GPAの3つの出力S1、S2、S3により制御されている。

- 11 -

およびT'3を遮断すると、保護回路は作動しなくなる。図示した実施例では、禁止トランジスタがPチャンネル型であるのに対し、シミュレーショントランジスタはNチャンネル型である。

シミュレーショントランジスタの寸法は、それらの消費(電流I)が、保護しようとする回路(図示していない)のメモリセルが読み出される(読み出し時の情報の機密を保護したい場合)ときの、あるいは書き込まれる(書き込み時の情報の機密を保護したい場合)ときのメモリセルの消費と同一であるような寸法であるのが望ましい。

機密情報の読み出しに対してROMを保護したい場合で、トランジスタが存在するかしないかどうかにより、記憶ビットの値“1”または“0”を定めるトランジスタによりメモリセルが形成されているとき、シミュレーショントランジスタの構成および寸法はメモリセルを形成するトランジスタの構成および寸法と同一であるのが望ましい。

メモリセルがフローティングゲートトランジスタであるEPROMまたはEEPROM中の書き込

各シミュレーションセルは、これを制御するフリップフロップの出力論理レベルに応じて、第1電流または第2電流のいずれかを消費するように構成されている。図示した実施例では、シミュレーションセルの主な構成要素は、各セルごとにトランジスタT1、T2、T3の各々である。シミュレーショントランジスタは、回路の給電端子VccとVssの間に接続され、これを制御するフリップフロップの出力レベルに応じて電流Iを消費またはゼロ電流消費すなわち電流を消費しない。

しかし、図面からわかるように、VccとVssの間ににおいて、トランジスタT1はトランジスタT'1と直列になり、トランジスタT2はトランジスタT'2と直列になり、トランジスタT3はトランジスタT'3と直列になるような好ましい形態に構成されている。トランジスタT'1、T'2およびT'3は禁止トランジスタであり、これらすべてが、保護信号が効果的に機能すべき瞬間を制御することのできる同一の禁止信号INHにより制御されている。禁止信号INHが、トランジスタT'1、T'2

- 12 -

みを保護したい場合には、シミュレーショントランジスタT1、T2、T3は、制御ゲートおよびフローティングゲートが短絡されたフローティングゲートトランジスタであるのが望ましい。これらのトランジスタの寸法は、保護しようとするメモリセルのトランジスタと同様であるのが望ましい。

セルの電流消費は、擬似乱数発生器GPAの出力S1、S2、S3により制御され、擬似乱数発生器GPAは、これらの出力S1、S2、S3にランダムに(実際は擬似乱数的に)“0”または“1”的ビットを与える。

しかし、シミュレーショントランジスタT1、T2、T3の制御は、共通クロックHLにより制御されるD型フリップフロップ、すなわち、BD1、BD2、BD3を介してなされる。共通クロックHLは保護したいメモリの読み出しおよび書き込みシーケンスを制御するクロックと同期化されているのが望ましい。

このようにして、出力S1、S2、S3で発生

- 13 -

- 14 -

する擬似乱数ビットは、このクロック信号 H L の立ち上がりエッジでのみ、すなわち、保護しようとするメモリセルの読出しままたは書き込みのための電流が消費される瞬間に、トランジスタに送られる。

第2図は、擬似乱数発生器 GPA の可能な構成の一例を示す。

この擬似乱数発生器は、N 個のカスケード接続された D 型フリップフロップ（各 D 型フリップフロップの出力は次の D 型フリップフロップの D 入力に接続される）により形成され、これらフリップフロップはすべて周波数 F の同一クロック信号により制御される。そして、これら D 型フリップフロップは、それぞれ P 1 および P 2 で示した 2 つの排他的 OR ゲートを介して 2 つのループを形成している。詳述するならば、第 1 フリップフロップの入力は、排他的 OR ゲート P 1 の出力に接続され、排他的 OR ゲート P 1 は、その入力として、第 2 フリップフロップの出力と、最後のフリップフロップ（N 番目のフリップフロップ）の出

力とを受けるように接続されている。更に、N-3 番目のフリップフロップの入力は、N-4 番目の出力ではなく、排他的 OR ゲート P 2 の出力に接続され、その排他的 OR ゲート P 2 は、その入力として、N-4 番目のフリップフロップの出力と最後の（N 番目の）フリップフロップの出力とを受けるように接続されている。

擬似乱数発生器の出力は、D 型フリップフロップの出力から取り出される。図示した実施例では、出力 S 1 、 S 2 、 S 3 はそれぞれ第 3 、第 4 および第 5 番目のフリップフロップの出力である。

後述する理由により、擬似乱数ビットを与える他の 2 つの出力 S a および S b も備えられる。これらの出力は、N-2 番目と N-1 番目のフリップフロップ、すなわちフリップフロップ列の最後より前の 2 つのフリップフロップの出力である。

第3図は、擬似乱数発生器に周波数 F のクロック信号を送る発振器 OSC と組み合わせた擬似乱数 GPA の発生器を示す。

発振器 OSC は、周波数制御発振器である。周

- 15 -

波数は、5 ビットの入力信号により制御される。これら 5 つのビットは、擬似乱数発生器 GPA 自体によりその出力 S 1 、 S 2 、 S 3 、 S a 、 S b を介して与えられた擬似乱数を表している。

従って、発振器の周波数は擬似乱数的に変化して、ビット S 1 、 S 2 、 S 3 の乱数特徴が高められる。

第4図は、可変周波数発振器 OSC の構成方法の一例を示す。

図示の発振器は、NOR ゲートを備え、このゲートの出力は第 1 インバータ I 1 の入力に接続される。第 1 インバータ I 1 の出力は、第 2 インバータ I 2 の入力に接続され、第 2 インバータ I 2 の出力は NOR ゲートの入力に接続されてループを構成している。NOR ゲートの他方の入力は、禁止動作ができることが望ましい場合に、単純に発振器を禁止する信号を受けるために使用される。

このカスケード接続された 3 つの反伝機能電子をループ状に接続することにより、発振が生じ、その周波数は、NOR ゲートの出力とアース (Vss)

- 16 -

との間と、第 1 インバータ I 1 の出力とアースとの間にそれぞれ挿入されたコンデンサにより調整される。

NOR ゲートの出力とアースの間には、3 つの並列接続のコンデンサ C 1 、 C 2 および C a が接続されているが、各コンデンサは、各コンデンサと直列接続された各トランジスタによって、切り離すことができる。各トランジスタ Q 1 、 Q 2 、 Q a は、擬似乱数発生器 GPA の出力 S 1 、 S 2 、 S a によりそれぞれ制御される。

同様に、インバータ I 1 とアース Vss との間に、2 つの並列接続のコンデンサ C 3 および C b が接続され、これらコンデンサの各々は、これと直列の各トランジスタ Q 3 、 Q b によって切り離すことができる。それぞれトランジスタ Q 3 および Q b は、擬似乱数発生器 GPA の各出力 S 3 、 S b によりそれぞれ制御される。

ビット S 1 、 S 2 、 S 3 、 S a 、 S b の状態によって、周波数 F は、可能な 32 個の周波数の内の 1 つの周波数をとる。従って、特に出力 S 1 、 S

- 17 -

-467-

- 18 -

2、S3に存在する擬似乱数ビットのシーケンスは、ランダムに変化する周波数で生成される。これは、出力S1、S2、S3で生成されるビットの乱数特徴、従って、本発明に従う保護回路の電流消費の乱数特徴を高める。このようにして、本発明により、機密情報の読出しまだは窃込みの動作時に集積回路の端子で消費される電流を読み取ってこの情報を検出する不正行為に対して、非常に高度の保護機能を達成することができる。

4・図面の簡単な説明

第1図は、本発明に従う保護回路のブロック図であり、第2図は、本発明に従う保護回路に使用できる擬似乱数発生器の一例を示し、第3図は、擬似乱数発生器が、該擬似乱数発生器の出力により周波数制御される発振器によりどのようにして制御されるかを示すブロック図であり、第4図は、第3図の発振器の詳細を示す図である。

(主な参照番号)

T1、T2、T3…トランジスタ、

T'1、T'2、T'3…禁止トランジスタ、

Vcc、Vss…給電端子、

GPA…擬似乱数発生器、

INH…禁止信号

HL…クロック信号、

OSC…発振器、

特許出願人 エスジエーエーストムソン エス.ア.

代理人 弁理士 越場 隆

- 19 -

- 20 -

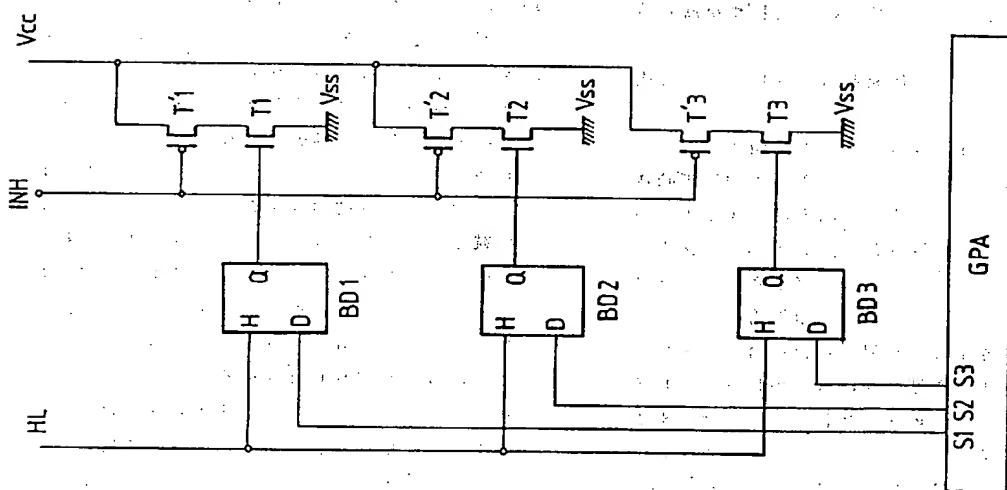


FIG. 1

FIG-2

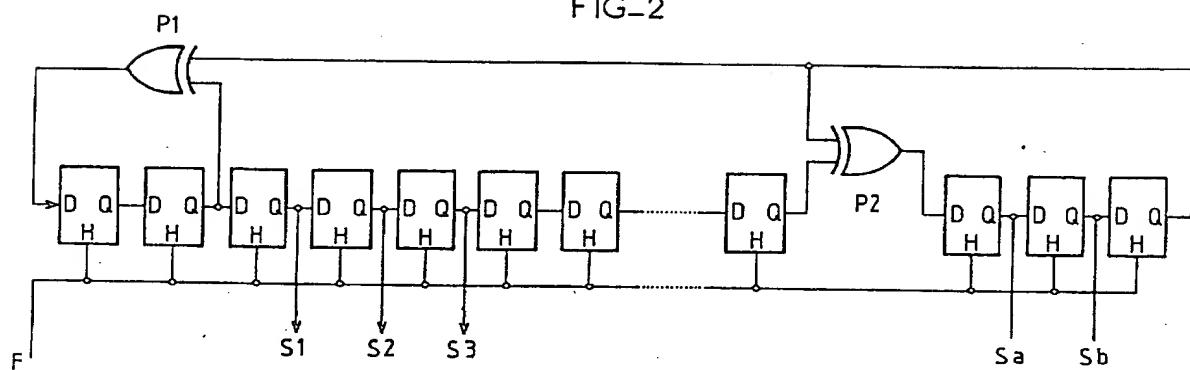


FIG-3

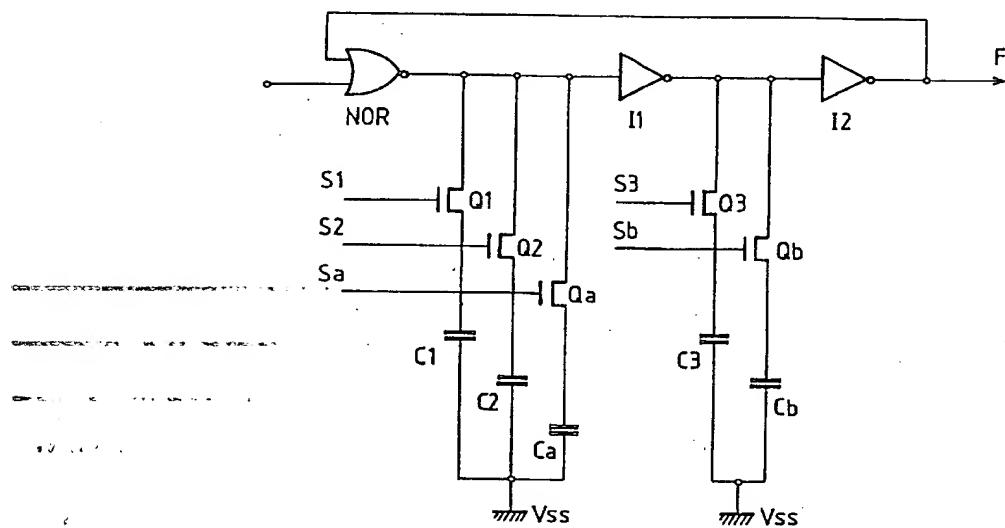
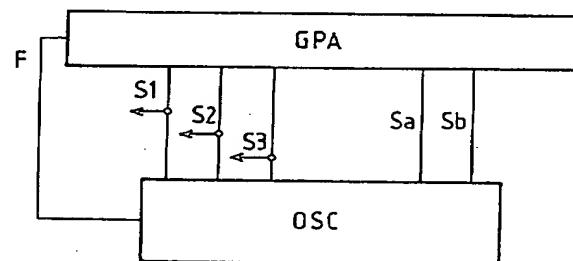


FIG-4

BESCHEIDSÜBERSETZUNG

Ausstellungsdatum: 09. 02. 2004

Zustellungsdatum: 13. 02. 2004

I. Die vorliegende Anmeldung entspricht in folgenden Punkten nicht Par. 36, Abs. 6 PG:

(1) Bei der Angabe "daß ein das Taktsignal bereitstellender Anschluß über jeweils ein steuerbares Schaltmittel mit dem Takteingang der jeweiligen Schaltungseinheiten verbunden ist" gemäß Anspruch 1 ist unklar, in welcher Verbindungsbeziehung der das Taktsignal bereitstellende Anschluß zu den Schaltungseinheiten steht. Daraufhin ist unklar, in welcher Weise der Betrieb der Schaltungseinheiten gesteuert wird. (Gegen Par. 36, Abs. 6, Ziff. 2 PG)

In der Beschreibung (vgl. Fig. 1) ist angegeben, daß mehrere Taktsignale über ein steuerbares Schaltmittel mit einer Schaltungseinheit verbunden werden, wobei durch die Umschaltung des steuerbaren Schaltmittels die Taktsignale mit verschiedenen Frequenzen der einzigen Schaltungseinheit zugeführt werden.

(2) Bei der Angabe "Zeitpunkt einer Schaltflanke" gemäß Anspruch 2 (sowie in der Beschreibung) ist unklar, was die "Flanke" ist. Daraufhin ist unklar, was mit der Angabe "Schaltflanke" gemeint ist. (Gegen Par. 36, Abs. 6, Ziff. 2 PG)

(3) Gegenüber den Angaben "eine erste Anzahl von Schaltungseinheiten (S1)", "eine zweite Anzahl von Schaltungseinheiten (S2)" und "weitere Anzahlen von Schaltungseinheiten (S3)" gemäß den Anspruch 3 sind die Elemente S1, S2 und S3 in der Beschreibung jeweils als eine Schaltungseinheit angegeben, so daß der Anspruch 3 mit der Beschreibung nicht übereinstimmt. (Gegen Par. 36, Abs. 6, Ziff. 1 PG)

(4) Im Anspruch 4 ist angegeben, daß "die Schaltmittel als (MP1, MP2, MP3, MP4) ausgebildet sind". Die eingeklammerte Angabe stellt jedoch lediglich eine Zusatzinformation dar, so daß die obige Angabe unklar ist. (Gegen Par. 36, Abs. 6, Ziff. 2 PG)

(5) Aus der Angabe "vor und/oder während und/oder nach" gemäß Anspruch 8 geht nicht klar hervor, in welcher Beziehung die Angaben "vor", "während" und "nach" zueinander stehen. (Gegen Par. 36, Abs. 6, Ziff. 2 PG)

II. Die vorliegende Anmeldung entspricht in folgenden Punkten

nicht Par. 36, Abs. 4 PG:

(1) Gegenüber der Angabe "Ein solches Ausführungsbeispiel ist in Figur 4 innerhalb einer strichlierten Linie dargestellt. Das in diesem Fall zu verwendende Taktsignal C1' ist durch einen ebenfalls strichlierten Pfeil angedeutet." in der Beschreibung (vgl. Seite 8, Zeilen 7 bis 9 des deutschen Textes) ist in Figur 4 unklar, in welcher Beziehung das Taktsignal C1' zu den anderen Schaltungen steht. Ferner ist unklar, wozu das Taktsignal C1' verwendet wird. (Es ist anzunehmen, daß als internes Taktsignal, das mit den Schaltungseinheiten verbunden wird, wird das Signal Clint verwendet, das auch in Figur 4 dargestellt ist.)

(2) Es ist anzunehmen, daß es sich bei der Angabe "nach der zweiten Taktperiode" aus der Angabe "Hier wird nach der zweiten Taktperiode ein Dummy-Takt eingeführt" in der Beschreibung (vgl. Seite 9, Zeilen 15 und 16 des deutschen Textes) um einen Schreibfehler handelt und es hier vielmehr "nach den zwei Taktperioden" heißen soll.

(3) Im unteren Teil der Figur 5 ist der Zustand des Taktsignals bei der Durchführung der Schaltungseinheit des Vorgangs I und der Schaltungseinheit des Vorgangs II dargestellt. Anhand dieser Figur ist bei dem Vorgang I+II trotz der umgeschalteten Schaltungseinheit die Breite des

Taktsignals (Frequenz des Taktsignals) nicht geändert.

Aufgrund des Blockschaltbildes gemäß Figur 1 können in den einzelnen Schaltungseinheiten Taktsignale mit verschiedenen Frequenzen eingegeben werden, während in Figur 5 nur dargestellt wird, daß in den Schaltungseinheiten der Vorgänge I, II die Taktsignale mit gleicher Frequenz stets eingegeben werden. (Obwohl die Frequenzen der Taktsignale geändert sind, werden an einem bestimmten Zeitpunkt in die Schaltungseinheiten der Vorgänge I, II unbedingt die Signale mit gleicher Frequenz eingegeben.)

Infolgedessen ist unklar, in welcher Beziehung das Blockschaltbild gemäß Figur 1 zu dem Zustand des Taktsignals gemäß Figur 5 steht.

Wenn bei der vorliegenden Erfindung an einem bestimmten Zeitpunkt in den gesamten Schaltungseinheiten stets die Taktsignale mit gleicher Frequenz eingegeben werden, ist die Erfindung gemäß Anspruch 3 in der Beschreibung nicht angegeben.

III. Die angemeldete Erfindung ist aufgrund folgender Vorveröffentlichung leicht herleitbar und daher gemäß Par. 29, Absatz 2 PG nicht schutzfähig:

Entgegenhaltung:

1. Jap. Pat.-Offenlegungsschrift Nr. 2-199561

Zu Anspruch 8:

Bei der Entgegenhaltung handelt es sich um ein Verfahren zum Betreiben einer Schaltung, bei dem während des Betriebs der getakteten zu schützenden Schaltung eine durch ein Zufallsignal bestimmte Anzahl von Taktsignalen einer Hilfsschaltungseinheit (T1, T2, T3) mit etwa gleichem Stromverbrauch wie die Schaltung zugeführt wird.

Zu den Ansprüchen 9 und 10:

Die Entgegenhaltung offenbart ein Verfahren zum Betreiben einer Schaltung, bei dem während des Betriebs der zu schützenden Schaltung für die Dauer von durch ein Zufallsignal bestimmten Zeitperioden (vgl. insbesondere Seite 5, oben rechts, Zeile 17 bis Seite 6, oben links, Zeile 9 sowie Fig. 3 und 4) die zu schützende Schaltung durch Zuführung eines Taktsignals in Betrieb genommen wird.

Darüber hinaus ist es bei der Steuerung des Betriebs einer integrierten Halbleiterschaltung üblich, einen Schaltungsteil zu aktivieren bzw. zu deaktivieren. Bei der Entgegenhaltung zur Steuerung des Betriebs einer zu schützenden Schaltung einen Schaltungsteil zu aktivieren

bzw. zu deaktivieren, kann daher von einem Fachmann leicht ausgeführt werden.

[Bei einer Verbesserungseingabe ist zu beachten, daß eine Ergänzung durch neue Merkmale unzulässig ist. (Dabei ist es erforderlich, im schriftlichen Widerspruch zu erläutern, aufgrund welcher Offenbarungen der ursprünglichen Beschreibung die Änderungen basieren.)]